PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-344445
(43)Date of publication of application : 29.11.2002

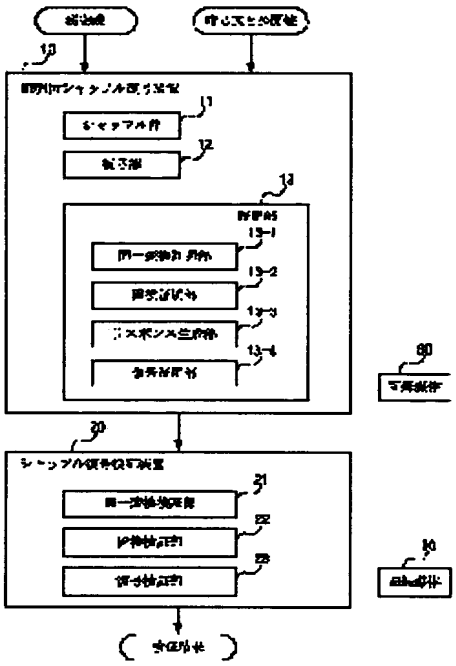
(51)Int.Cl. H04L 9/32
G09C 1/00

(21)Application number : 2001-149331
(22)Date of filing : 18.05.2001

(71)Applicant : NEC CORP
(72)Inventor : FURUKAWA JUN

(54) SHUFFLE-DECODING SYSTEM WITH CERTIFICATION AND METHOD THEREFOR, AND SHUFFLE DECODING VERIFICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a shuffle decoding system with certification capable of efficiently processing calculation quantity and certification statement quantity.
SOLUTION: This system is provided with a shuffle-decoding device, having certification for generating a shuffle decoding statement and a shuffle decoding certification statement and a shuffle-decoding verifying device for verifying the shuffle decoding processing, by referring to the generated shuffle decoding statement and the shuffle decoding certification statement. The shuffle-decoding device with certification accepts the input of a plurality of cryptographic statements and a public key and the secret key of the decoding; generates the shuffled cryptographic statements by enciphering the cryptographic statements with the public key by exchanging the order of the cryptographic statement; generates shuffle decoded statement statements by decoding the shuffled cryptographic statements with the secret key; generates a response to be referred to when executing certification, and generates a certification statement for certifying the validity of the exchange of the order of the cryptographic statements, the encipherment, and the decoding for generating the shuffle decoded statements based on the response; and output the respective generated certification statements and responses as shuffle-decoding certification statements.



LEGAL STATUS

[Date of request for examination] 12.02.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－344445
（P2002－344445A）
(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/32		Ｇ０９Ｃ	1/00	６４０Ｃ　５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０	Ｈ０４Ｌ	9/00	６７５Ｃ

審査請求　未請求　請求項の数19　ＯＬ　（全 17 頁）

(21)出願番号　特願2001－149331(P2001－149331)

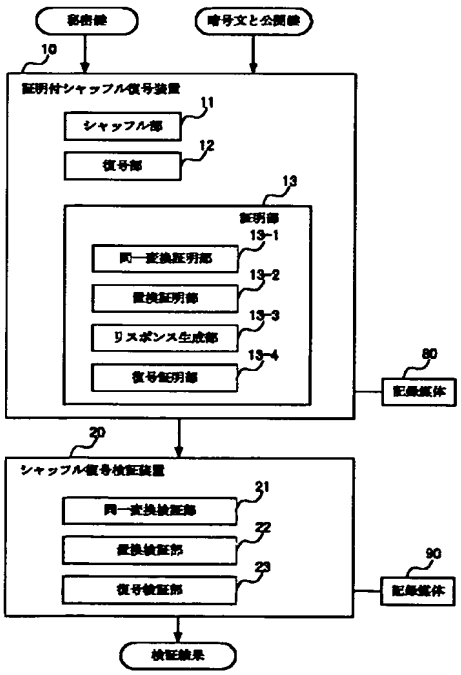
(22)出願日　平成13年５月18日(2001.5.18)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　古川　潤
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100093595
弁理士　松本　正夫

Ｆターム(参考)　5J104 AA18 JA29 KA08 NA02 NA09 NA10

(54)【発明の名称】　証明付シャッフル復号システムと証明付シャッフル復号方法、シャッフル復号検証方法

(57)【要約】　（修正有）
【課題】　計算量と証明文量を効率良く処理する証明付シャッフル復号システムの提供。
【解決手段】　シャッフル復号文を生成し、且つシャッフル復号証明文を生成する証明付シャッフル復号装置と、生成されたシャッフル復号文とシャッフル復号証明文とを参照し、シャッフル復号処理の検証を行うシャッフル復号検証装置を備え、証明付シャッフル復号装置は、複数の暗号文と、公開鍵と復号の秘密鍵との入力を受け付け、暗号文の順番を入れ替えて公開鍵により暗号化したシャッフル済み暗号文を、秘密鍵により復号してシャッフル復号文を生成し、証明において参照するリスポンスを生成し、リスポンスに基づいて、シャッフル復号文を生成する為の順番の入れ替えと暗号化と復号とにおけるそれぞれの正当性を証明する証明文を生成し、生成された各証明文とリスポンスとを、シャッフル復号証明文として出力する事を特徴とする。



1

【特許請求の範囲】

【請求項１】　複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号装置において、

前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、

前記証明において参照するリスポンスを生成し、

前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、

前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力することを特徴とする証明付シャッフル復号装置。

【請求項２】　前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル部と、

前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号部と、

前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明部を備えることを特徴とする請求項１に記載の証明付シャッフル復号装置。

【請求項３】　前記証明部は、

前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明部と、

前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明部と、

前記同一変換証明部と置換証明部に対する前記リスポンスを生成するリスポンス生成部と、

前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明部を備え、

前記同一変換証明部と、前記置換証明部と、前記リスポンス生成部と、前記復号証明部により生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする請求項２に記載の証明付シャッフル復号装置。

2

【請求項４】　複数の暗号文をシャッフル復号して生成されたシャッフル復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証装置において、

前記シャッフル復号証明文は、

証明において参照するリスポンスと、

前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とするシャッフル復号検証装置。

【請求項５】　前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証部と、

前記シャッフル復号証明文の入力と前記同一変換検証部で生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証部と、

前記シャッフル復号証明文と前記同一変換検証部で生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証部とを備え、

前記同一変換検証部と、前記置換検証部と、前記復号検証部のそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする請求項４に記載のシャッフル復号検証装置。

【請求項６】　複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号方法において、

前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、

前記証明において参照するリスポンスを生成し、

前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、

前記生成された各証明文と前記リスポンスとを、前記シ

ャッフル復号証明文として出力することを特徴とする証明付シャッフル復号方法。

【請求項７】　前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフルステップと、

前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号ステップと、

前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明ステップを備えることを特徴とする請求項６に記載の証明付シャッフル復号方法。

【請求項８】　前記証明ステップは、

前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明ステップと、

前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明ステップと、

前記同一変換証明ステップと置換証明ステップに対する前記リスポンスを生成するリスポンス生成ステップと、

前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明ステップを備え、

前記同一変換証明ステップと、前記置換証明ステップと、前記リスポンス生成ステップと、前記復号証明ステップにおいて生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする請求項７に記載の証明付シャッフル復号方法。

【請求項９】　複数の暗号文をシャッフル復号して生成されたシャッフル復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証方法において、

前記シャッフル復号証明文は、

証明において参照するリスポンスと、

前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とするシャッフル復号検証方法。

【請求項１０】　前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証ステップと、

前記シャッフル復号証明文の入力と前記同一変換検証ステップで生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証ステップと、

前記シャッフル復号証明文と前記同一変換検証ステップで生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証ステップとを備え、

前記同一変換検証ステップと、前記置換検証ステップと、前記復号検証ステップのそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする請求項９に記載のシャッフル復号検証方法。

【請求項１１】　複数の暗号文をシャッフル復号して生成したシャッフル復号文の、前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成し、前記シャッフル復号証明文に基づいて前記シャッフル復号の処理が正しく行われたことを検証する証明付シャッフル復号システムにおいて、

前記複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号証明文を生成する証明付シャッフル復号装置と、

生成された前記シャッフル復号文と、当該シャッフル復号文の前記シャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証装置を備え、

前記証明付シャッフル復号装置は、

前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、

前記証明において参照するリスポンスを生成し、

前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、

前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力することを特徴とする証明付シャッフル復号システム。

【請求項１２】　前記証明付シャッフル復号装置は、

前記複数の暗号文と前記公開鍵との入力を受けて、前記

複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル部と、
前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号部と、
前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明部を備えることを特徴とする請求項１１に記載の証明付シャッフル復号システム。

【請求項１３】　前記証明付シャッフル復号装置の前記証明部は、
前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明部と、
前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明部と、
前記同一変換証明部と置換証明部に対する前記リスポンスを生成するリスポンス生成部と、
前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明部を備え、
前記同一変換証明部と、前記置換証明部と、前記リスポンス生成部と、前記復号証明部により生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする請求項１２に記載の証明付シャッフル復号システム。

【請求項１４】　前記シャッフル復号検証装置は、
前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証部と、
前記シャッフル復号証明文の入力と前記同一変換検証部で生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証部と、
前記シャッフル復号証明文と前記同一変換検証部で生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証部とを備え、
前記同一変換検証部と、前記置換検証部と、前記復号検証部のそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする請求項１１から請求項１３のいずれか一つに記載の証明付シャッフル復号システム。

【請求項１５】　コンピュータを制御することにより、複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号プログラムにおいて、
前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、
前記証明において参照するリスポンスを生成し、
前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、
前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力する処理を実行させることを特徴とする証明付シャッフル復号プログラム。

【請求項１６】　前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル処理と、
前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号処理と、
前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明処理を実行させることを特徴とする請求項１５に記載の証明付シャッフル復号プログラム。

【請求項１７】　前記証明処理は、
前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明処理と、
前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明処理と、
前記同一変換証明処理と置換証明処理に対する前記リスポンスを生成するリスポンス生成処理と、
前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号

証明処理と、
前記同一変換証明処理と、前記置換証明処理と、前記リスポンス生成処理と、前記復号証明処理において生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力する処理を実行させることを特徴とする請求項１６に記載の証明付シャッフル復号プログラム。
【請求項１８】　コンピュータを制御することにより、複数の暗号文をシャッフル復号して生成されたシャッフル復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証プログラムにおいて、
前記シャッフル復号証明文は、
証明において参照するリスポンスと、
前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とするシャッフル復号検証プログラム。
【請求項１９】　前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証処理と、
前記シャッフル復号証明文の入力と前記同一変換検証処理で生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証処理と、
前記シャッフル復号証明文と前記同一変換検証処理で生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証処理と、
前記同一変換検証処理と、前記置換検証処理と、前記復号検証処理のそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定する処理を実行させることを特徴とする請求項１８に記載のシャッフル復号検証プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、匿名通信路の構成等において使われる、証明付シャッフル及び証明付復号を処理する証明付シャッフル復号システムと証明付シャッフル復号方法、シャッフル復号検証方法に関する。
【０００２】
【従来の技術】［従来の証明付シャッフル］従来の証明付シャッフルの技術には、例えば、特願２０００－０５９０９１号（以下、文献１）に記載された従来技術がある。
【０００３】図６は、文献１に記載された従来技術の構成を示す図である。なお、以下各図面中においては、合流する矢印は、矢印の元の側における情報が全て集まって矢印の先へ送られることを意味し、分岐する矢印は、矢印の元の側の情報の全て又は一部がそれぞれの矢印の先へ送られることを意味する。
【０００４】また、本明細書におけるシャッフルは、文献１においては再暗号シャッフルと呼んでいる。ここで、シャッフルとは、入力された暗号文をその順序を入れ替えて再び暗号化することである。
【０００５】図６においては、まず、暗号文と公開鍵１００がシャッフルステップ１０１に入力されてシャッフルされる。この時入力された暗号文１００とシャッフルを特定する情報であるシャッフル情報１０２が同一変換証明ステップ１０３に送られ、シャッフル情報１０２が置換証明ステップ１０４に送られる。同一変換証明ステップ１０３は、同一変換証明文１０５を生成し出力すると同時に、証明文生成に使用した乱数１０６を置換証明ステップ１０４に送る。置換証明ステップ１０４は置換証明文１０７を出力する。リスポンス生成ステップ１０８には、同一変換証明文１０５と置換証明文１０４と暗号文と公開鍵１００とシャッフル済み暗号文１０９とを入力し、同一変換証明文１０５と置換証明文１０４と暗号文とにリスポンスを加えてシャッフル証明文１１０を生成し出力する。
【０００６】同一変換証明文１０５は、リスポンスと合さって、入力文の順番の入れ替えや暗号化である暗号文の変換内容の知識を持っていることの証明であると同時に、入力される暗号文が複数の整数の要素となる場合はそれぞれの要素が同じ順番の入れ替えと対応する暗号化の処理とを受けたことの証明でもある。置換証明文１０７は、リスポンスと合さって、入力される暗号文に対しての、順番の入れ替えが正しくなされたことの証明である。
【０００７】このシャッフルの処理が正当であることを証明するために、文献１では同一変換証明ステップと置換証明ステップの二つの証明ステップを用いている。この証明対象の分割により文献１ではシャッフル証明文生成の効率化を達成している。
【０００８】［従来の証明付復号］従来の証明付復号の技術には、例えば、特開平０８－２６３５７５号公報（以下、文献２）に開示された従来技術がある。
【０００９】図７は、文献２に開示された従来技術の構成を示す図である。図７を参照すると、まず、シャッフ

ル済み暗号文２００と秘密鍵２０１とが、復号ステップ２０３に入力されて復号される。この時入力されたシャッフル済み暗号文２００と秘密鍵２０１と、複合されて得られた復号文２０４とが、復号証明ステップ２０５に送られる。復号証明ステップ２０５は、これらの情報より復号証明文２０６を出力する。

【００１０】ここで、復号とは、暗号文を分散所持されている秘密鍵の一部を使って、部分的に暗号文を復号することであり、秘密鍵の一部を全て用いて復号を繰り返すと完全な復号がなされる。

【００１１】［従来の技術による、証明付シャッフル復号方法］文献１の証明付シャッフルの技術と、文献２の証明付復号の技術とを合わせることにより、証明付シャッフル復号方法を構成することができる。

【００１２】図８は、文献１と文献２の従来技術を単純につなげることにより構成された証明付シャッフル復号方法を示す図である。この方法では、シャッフル済み暗号文３０４がシャッフル復号証明文３１６に含まれていることと、シャッフル済み暗号文３０４が復号証明ステップに入力されることと、リスポンス生成ステップからの入力がないこととが特徴である。

【００１３】

【発明が解決しようとする課題】上述したように従来の技術では、以下に述べるような問題点があった。

【００１４】入力された暗号文をシャッフルし、かつそのシャッフルされた結果に復号を施して復号文を出力し、更にその処理の正当性証明文を生成して出力する方式を考える。これは、前述のように、文献１と文献２の従来技術を組み合わせることにより匿名通信路を構成することができるが、この手法では、不要な情報であるシャッフル済み暗号文が正当性の証明のために必要となり、これを出力する必要がある。暗号文の数が多い場合等、このように不要なシャッフル済み暗号文を出力することは、証明文量を増大させ通信の効率を悪くする。

【００１５】また、文献２の従来技術では、証明文生成のために計算量の大きい冪乗剰余演算を暗号文数に比例して行わなければならない。そのためにシャッフル復号の効率を悪くしている。

【００１６】本発明の第１の目的は、上記従来技術の欠点を解決し、文献１と文献２を組み合わせた方式であって、シャッフル済み暗号文を出力する必要がなく、かつ計算量と証明文量を共に少なく抑え効率の良い証明付シャッフル復号システムと証明付シャッフル復号方法、シャッフル復号検証方法を提供することである。

【００１７】本発明の第２の目的は、上記従来技術の欠点を解決し、冪乗剰余演算の回数及び計算量を大きく削減し、更なる高速化を実現する証明付シャッフル復号システムと証明付シャッフル復号方法、シャッフル復号検証方法を提供することである。

【００１８】

【課題を解決するための手段】上記目的を達成するため本発明の証明付シャッフル復号装置は、複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号装置において、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するリスポンスを生成し、前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力することを特徴とする。

【００１９】請求項２の本発明の証明付シャッフル復号装置は、前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル部と、前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号部と、前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明部を備えることを特徴とする。

【００２０】請求項３の本発明の証明付シャッフル復号装置は、前記証明部は、前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明部と、前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明部と、前記同一変換証明部と置換証明部に対する前記リスポンスを生成するリスポンス生成部と、前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明部を備え、前記同一変換証明部と、前記置換証明部と、前記リスポンス生成部と、前記復号証明部により生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする。

【００２１】請求項４の本発明のシャッフル復号検証装置は、複数の暗号文をシャッフル復号して生成されたシャッフル復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル

復号検証装置において、前記シャッフル復号証明文は、証明において参照するリスポンスと、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とする。

【００２２】請求項５の本発明のシャッフル復号検証装置は、前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証部と、前記シャッフル復号証明文の入力と前記同一変換検証部で生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証部と、前記シャッフル復号証明文と前記同一変換検証部で生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証部とを備え、前記同一変換検証部と、前記置換検証部と、前記復号検証部のそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする。

【００２３】請求項６の本発明の証明付シャッフル復号方法は、複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号方法において、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するリスポンスを生成し、前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力することを特徴とする。

【００２４】請求項７の本発明の証明付シャッフル復号方法は、前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフルステップと、前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号ステップと、

前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明ステップを備えることを特徴とする。

【００２５】請求項８の本発明の証明付シャッフル復号方法は、前記証明ステップは、前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明ステップと、前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明ステップと、前記同一変換証明ステップと置換証明ステップに対する前記リスポンスを生成するリスポンス生成ステップと、前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明ステップを備え、前記同一変換証明ステップと、前記置換証明ステップと、前記リスポンス生成ステップと、前記復号証明ステップにおいて生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする。

【００２６】請求項９の本発明のシャッフル復号検証方法は、複数の暗号文をシャッフル復号して生成されたシャッフル復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証方法において、前記シャッフル復号証明文は、証明において参照するリスポンスと、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とする。

【００２７】請求項１０の本発明のシャッフル復号検証方法は、前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証ステップと、前記シャッフル復号証明文の入力と前記同一変換検証ステップで生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証ステップと、前記シャッフル復号証明文と前記同一変換検証ステップで生成されたチャレンジとの入力を受け

て、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証ステップとを備え、前記同一変換検証ステップと、前記置換検証ステップと、前記復号検証ステップのそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする。

【００２８】請求項１１の本発明の証明付シャッフル復号システムは、複数の暗号文をシャッフル復号して生成したシャッフル復号文の、前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成し、前記シャッフル復号証明文に基づいて前記シャッフル復号の処理が正しく行われたことを検証する証明付シャッフル復号システムにおいて、前記複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号証明文を生成する証明付シャッフル復号装置と、生成された前記シャッフル復号文と、当該シャッフル復号文の前記シャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証装置を備え、前記証明付シャッフル復号装置は、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するリスポンスを生成し、前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力することを特徴とする。

【００２９】請求項１２の本発明の証明付シャッフル復号システムは、前記証明付シャッフル復号装置は、前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル部と、前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号部と、前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明部を備えることを特徴とする。

【００３０】請求項１３の本発明の証明付シャッフル復号システムは、前記証明付シャッフル復号装置の前記証明部は、前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明部と、前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明部と、前記同一変換証明部と置換証明部に対する前記リスポンスを生成するリスポンス生成部と、前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明部を備え、前記同一変換証明部と、前記置換証明部と、前記リスポンス生成部と、前記復号証明部により生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする。

【００３１】請求項１４の本発明の証明付シャッフル復号システムは、前記シャッフル復号検証装置は、前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証部と、前記シャッフル復号証明文の入力と前記同一変換検証部で生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証部と、前記シャッフル復号証明文と前記同一変換検証部で生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証部とを備え、前記同一変換検証部と、前記置換検証部と、前記復号検証部のそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする。

【００３２】請求項１５の本発明の証明付シャッフル復号プログラムは、コンピュータを制御することにより、複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号プログラムにおいて、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するリスポンスを生成し、前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力する処理を実行させることを特徴とする。

【００３３】請求項１８の本発明のシャッフル復号検証プログラムは、コンピュータを制御することにより、複数の暗号文をシャッフル復号して生成されたシャッフル

復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証プログラムにおいて、前記シャッフル復号証明文は、証明において参照するリスポンスと、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とする。

【００３４】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【００３５】［証明付シャッフル復号方法］本発明の証明付シャッフル復号においては、まず、暗号文と公開鍵と秘密鍵とを入力して、その暗号文と公開鍵からシャッフル済み暗号文を生成し、そのシャッフル済み暗号文を秘密鍵により復号して復号文を生成する。

【００３６】次に、証明付シャッフル方法（証明付暗号シャッフル方法）を用いて、シャッフル済み暗号文とシャッフル証明文を生成する。この証明付シャッフルの処理は、例えば、文献１に記載された従来の技術を持ちいることができる。但し、本発明においては、証明文生成時のチャレンジ（文献１では挑戦値と記述）を生成する時に、シャッフル済み暗号文の代わりに復号文を用いる。

【００３７】次に、検証仮定にてシャッフル済み暗号文の代わりに復号文を用いた場合に生じることによる検証式の差分を生成し、これをシャッフル証明文に加える。

【００３８】次に、前記差分が正当に作成されたことの証明文を、復号証明文として生成する。前記シャッフル証明文と復号証明文を合わせてシャッフル復号証明文とし、この復号文とシャッフル復号証明文とを出力する。

【００３９】［シャッフル復号検証方法］本発明のシャッフル復号検証においては、まず、暗号文と公開鍵と復号文とシャッフル復号証明文とを入力する。ここで本発明では、文献１のシャッフル検証におけるシャッフル済み暗号文の代わりに、復号文を入力して検証を行う。但し、シャッフル復号証明文に含まれる「検証仮定において、シャッフル済み暗号文の代わりに復号文を用いたために生じる検証式の差分」を利用して、検証式を修正して用いる。次に、前記差分の正当性を検証する。二つの検証（復号文を用いたシャッフル検証と、検証式の差分の正当性の検証）の結果が共に「正当」であれば、シャッフル復号の検証結果として「正当」を、そうでなければ「不当」を出力する。

【００４０】図１は、本発明の一実施の形態による証明付シャッフル復号システムの構成を示すブロック図である。図１を参照すると、本実施の形態の証明付シャッフル復号システムは、証明文を生成する側の装置である証明付シャッフル復号装置１０と、証明文を基に検証を行う側の装置であるシャッフル復号検証装置２０を備えている。

【００４１】証明付シャッフル復号装置１０は、シャッフル部１１、復号部１２、証明部１３を備えている。

【００４２】シャッフル部１１は、複数の暗号文と公開鍵との入力を受けて、入力された複数の暗号文の順番を入れ替えて、その結果を公開鍵により暗号化した複数のシャッフル済み暗号文を生成する。

【００４３】復号部１２は、シャッフル部１１により生成された複数のシャッフル済み暗号文と、秘密鍵の入力を受けて、シャッフル済み暗号文を秘密鍵により復号した複数の復号文を生成し出力する。

【００４４】証明部１３は、複数の暗号文と公開鍵と秘密鍵とに基づいて証明文を生成する。証明部１３は、更に同一変換証明部１３－１、置換証明部１３－２、リスポンス生成部１３－３、復号証明部１３－４を備えている。

【００４５】同一変換証明部１３－１は、シャッフル部１１による順番の入れ替えの前後の対応関係と、暗号化に使った乱数とを知っていることを証明する（ゼロ知識証明を行う）証明文を生成する。また、同一変換証明部１３－１は、入力される暗号文が複数の整数の要素からなる場合には、それぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明するための証明文も生成する。

【００４６】置換証明部１３－２は、入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する。リスポンス生成部１３－３は、同一変換証明部１３－１と置換証明部１３－２に対するリスポンスを生成する。復号証明部１３－４は、シャッフル済み暗号文が、秘密鍵を用いて正しく復号されて復号文が生成されたことを証明する証明文を生成する。

【００４７】そして、証明付シャッフル復号装置１０は、同一変換証明部１３－１、置換証明部１３－２、リスポンス生成部１３－３、復号証明部１３－４により生成された証明文とリスポンスの全てを、シャッフル復号の証明文として出力する。

【００４８】シャッフル復号検証装置２０は、同一変換検証部２１、置換検証部２２、復号検証部２３を備えている。

【００４９】同一変換検証部２１は、シャッフル復号証明文と暗号文と公開鍵と復号文の入力を受けて、順番の入れ替え及び暗号化である暗号文の変換内容の知識を持っていることを検証する。また、同一変換検証部２１は、入力される暗号文が複数の整数の要素となる場合は、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けたことを検証する。そして、同一変換検証部

２１は、検証結果を「正当」又は「不当」として出力し、またチャレンジ（挑戦値）を生成し出力する。

【００５０】置換検証部２２は、シャッフル復号証明文と同一変換検証部２１により生成されたチャレンジの入力を受けて、入力される暗号文に対しての順番の入れ替えが正しくなされたことを検証し、その検証結果を「正当」又は「不当」として出力する。

【００５１】復号検証部２３は、シャッフル復号証明文と同一変換検証部２１により生成されたチャレンジの入力を受けて、シャッフル済み暗号文が秘密鍵を用いて正しく復号されて復号文が生成されたことを検証し、その検証結果を「正当」又は「不当」として出力する。

【００５２】シャッフル復号検証装置２０は、この同一変換検証部２１、置換検証部２２、復号検証部２３のそれぞれの検証結果の全てが「正当」でる場合には、シャッフル復号文が入力された暗号文を正しくシャッフル復号した結果であると判定し、その判定結果を「正当」と出力する。また、この検証結果の内の一つでも「不当」である場合には、その判定結果を「不当」と出力する。

【００５３】以下、本実施の形態においては、Ｅｌｇａｍａｌ暗号を用いる実施例を用いて本発明を説明する。以下では、本発明にて前提となる事項から順に説明していく。

【００５４】［Ｅｌｇａｍａｌ暗号方式］Ｅｌｇａｍａｌ暗号方式は、公開鍵暗号系に属する暗号方式である。最初に関係

$p=kq+1$

を満たしている二つの素数ｐ、ｑを定める。これらの素数はＥｌＧａｍａｌドメインパラメタと呼ばれる。秘密鍵

$x \in_R Z_q$

をZ_qの要素から選ぶ。次に公開鍵

（g_0、m_0）

を位数ｑのZ^*_pの要素で、

$m_0 = g_0^x \bmod p$

この式を満たすものとして選ぶ。

【００５５】Z^*_pの要素である平文

$P \in Z^*_p$

を暗号化するには、秘密に乱数

$s \in_R Z_q$

を生成して暗号文を

$(G, M) = (g_0^s, m_0^s P) \bmod p$

と計算する。この暗号文を復号するには秘密鍵

$x \in_R Z_q$

を用いて、

$P' = M / G^x \bmod p$

と計算する。復号文Ｐ’は、平文Ｐに一致する。

【００５６】ここで、秘密鍵

$x \in_R Z_q$

が分散所持されている場合を考える。すなわち、ｘがｎ個のx_j（ｊ＝１、…、ｎ）により別個に分散所持され、

$x = (x_1 + \cdots + x_n) \bmod q$

が成り立つ場合である。本明細書では、このx_j（ｊ＝１、…、ｎ）を復号用の秘密鍵と呼ぶこととする。

【００５７】この時暗号文を完全に復号するには、数１の式により、Ｍを各復号用の秘密鍵を用いて計算した値で順に割っていく復号操作を、全てのx_j（ｊ＝１、…、ｎ）に関して行う。ただし、本実施例では１つの復号用の秘密鍵しか扱わないため、これをｘ’と表す。

【数１】

$$G^{x_j} \bmod p$$

【００５８】［暗号文］入力されるｎ個の暗号文を、数２により示されるものとする。それぞれの暗号文の各要素は位数ｑのZ^*_pの元である。

【数２】

$$(g_i, m_i) \quad i=1,\ldots,n$$

【００５９】［復号文］出力されるｎ個の復号文を、、数２により示されるものとする。それぞれの復号文の各要素は位数ｑのZ^*_pの元である。

【数３】

$$(\tilde{g}_i, \tilde{m}_i) \quad i=1,\ldots,n$$

【００６０】これらは、数４に示されるｎ個の暗号文の順番を入れ替えた後に、復号用の秘密鍵で復号したものである。

【数４】

$$(g_i, m_i) \quad i=1,\ldots,n$$

【００６１】［挑戦値生成関数］挑戦値生成関数について説明する。図５のフローチャートに示される、次のような４ステップからなる対話的証明プロトコルを考える。

【００６２】まず、証明者が検証者に証明したいことに関するコミットメントを送る（ステップＡ１）。そして、検証者が挑戦値を証明者に送る（ステップＡ２）。そして、証明者は挑戦値に対して、応答を送る（ステップＡ３）。そして、検証者はこれらコミットメント、挑戦値、応答内容から証明の真偽を確認する（ステップＡ４）。

【００６３】このような対話的証明プロトコルでは、証明者がどのような挑戦値に対しても適切な応答を送り返すことができることが、証明となる。ステップＡ２において、検証者の代わりに挑戦値を生成する関数を用いることで、上記対話的証明プロトコルを非対話的プロトコルに変換することができる。

【００６４】すなわち、図２のフローチャートに示されるように、まず証明者が、検証者に証明したいことに関

するコミットメントを生成する（ステップＢ１）。そして、コミットメントと証明したい内容を関数に入力して、関数の出力を挑戦値とする（ステップＢ２）。そして、証明者は、挑戦値に対して応答を生成し、以上の生成された各データを検証者に送る（ステップＢ３）。そして、検証者は、証明者から送られたこれらコミットメント、挑戦値、応答内容から証明の真偽を確認する（ステップＢ４）。

【００６５】以上のように本発明の証明プロトコルでは、ステップＢ１からステップＢ３までの間、証明者は検証者と対話することなく証明を生成している。

【００６６】上記挑戦値を生成する関数を挑戦値生成関数と呼び、これを数５により示す。

【００６７】

【数５】

$$H_i(*) \quad i=1,\ldots,n$$

挑戦値生成関数の出力は、ｎ＋１個の“１”、“０”でないｑ以下の整数である。また、この関数は入出力間や出力の異なる成分間の関係を、計算量的に意図して引数を決定できない関数とする。

【００６８】挑戦値生成関数の具体的な構成方法の例としては、数６の式があげられる。

【数６】

$$H_i(x) = \mathrm{Hash}((\mathrm{Hash}(x))^i \bmod q) \bmod q$$

【００６９】［置換行列］置換行列について説明する。ここで「置換行列」を、各行各列に“０”でない成分が唯一存在し、その“０”である値をZ_q上の“１”とするｎ行×ｎ列の正方行列と定義する。例として、数７の行列があげられる。

【数７】

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

【００７０】［シャッフル行列］シャッフル行列を定義する。「シャッフル行列」を、ｎ＋１行×ｎ＋１列の行列

$\{A_{\mu,\nu}\}$　（μ、ν＝０、…、ｎ）

であって、その成分が、$\{A_{i,j}\}$　（ｉ、ｊ＝１、…、ｎ）：ｎ行×ｎ列の置換行列

$A_{0,j}$　、$A_{i,0}$　、$A_{0,0}$　$\in_R Z_q$　（ｉ、ｊ＝１、…、ｎ）

を成すものと定義する。

【００７１】［証明付シャッフル復号］本発明の一実施例を成す証明付シャッフル復号方法について、図８を参照して説明する。

【００７２】［シャッフルステップ４０２］暗号文と公開鍵４０１

（g_i、m_i）、（g_0、m_0）：（ｉ＝１、…、ｎ）

が入力される。

【００７３】次に、シャッフルステップ４０２にて任意のシャッフル情報４０３

$A_{0,j}$　$\in_R Z_q$　（ｊ＝１、…、ｎ）

$A_{i,j}$　：置換行列（ｉ、ｊ＝１、…、ｎ）

を準備する。

【００７４】次に、シャッフル済み暗号文４０４である数８の各変数の値を、数９の式により計算する。そして、シャッフルステップ４０２は、シャッフル情報４０３とシャッフル済み暗号文４０４とを出力する。

【数８】

$$(\bar{g}_i, \bar{m}_i) \quad i=1,\ldots,n$$

【数９】

$$\bar{g}_i = \prod_{\nu=0}^{n} g_\nu^{A_{\nu i}} \bmod p \quad i=1,\ldots,n$$

$$\bar{m}_i = \prod_{\nu=0}^{n} m_\nu^{A_{\nu i}} \bmod p \quad i=1,\ldots,n$$

【００７５】［復号ステップ４０５］シャッフル済み暗号文４０４と復号用の秘密鍵４００とが入力される。次に、復号文４０６を数１０の式により計算して出力する。

【数１０】

$$\tilde{g}_i = \bar{g}_i \bmod p \quad i=1,\ldots,n$$

$$\tilde{m}_i = \bar{g}_i^{-x'} \bar{m}_i \bmod p \quad i=1,\ldots,n$$

【００７６】［同一変換証明ステップ４０７］シャッフル情報４０３と暗号文４０１と公開鍵４０１が入力される。次に、任意の乱数４０８

$A_{\mu,0}$　$\in_R Z_q$　（μ＝０、…、ｎ）

を準備して、コミットメンとの一部である数１１の各変数の値を、数１２の式により計算して、同一変換証明文４０９として出力する。

【数１１】

$$(\tilde{g}_0, \tilde{m}_0)$$

【数１２】

$$\tilde{g}_0 = \prod_{\nu=0}^{n} g_\nu^{A_{\nu 0}} \bmod p$$

$$\tilde{m}_0 = \prod_{\nu=0}^{n} m_\nu^{A_{\nu 0}} \bmod p$$

【００７７】［置換証明ステップ４１０］シャッフルステップ４０２で生成されたシャッフル情報４０３と同一変換証明ステップ４０７で生成された乱数４０８とから

21

なるシャッフル行列
$A_{\mu,\nu} \mod q$ （μ、$\nu=0$、…、n）
が入力される。

【００７８】次に、（0、1ではない）任意の乱数 ＊
＊σ、ρ、ρ'、$\lambda_\mu \in_R Z_q$ （$\mu=0$、…、n）
$g=g_0$
を準備して、数１３を計算する。

【数１３】

$$\dot{\phi}_i = \sum_{j=1}^{n}\left(3A_{j0}+\rho'\lambda_j\right)A_{ji} \mod q \qquad i=1,\ldots,n$$

$$\phi_i = \sum_{j=1}^{n}\left(3A_{j0}+2\rho'\lambda_j\right)A_{j0}A_{ji}+\rho A_{0i} \mod q \qquad i=1,\ldots,n$$

$$\phi_0 = \sum_{j=1}^{n}\left(A_{j0}+\rho'\lambda_j\right)A_{j0}A_{j0}+\rho'\lambda_0+\rho A_{00} \mod q$$

$$\psi_i = \sum_{j=1}^{n}2A_{j0}A_{ji}+\sigma A_{0i} \mod q \qquad i=1,\ldots,n$$

$$\psi_0 = \sum_{j=1}^{n}A_{j0}A_{j0}+\sigma A_{00} \mod q$$

$$v=g^{\rho},\ v'=g^{\rho'},\ \dot{v}_0=g^{\phi_0},\ \dot{v}_i=g^{\phi_i},$$
$$w=g^{\sigma},\ \dot{w}_0=g^{\psi_0},\ \dot{w}_i=g^{\psi_i},$$
$$\dot{u}_i=g^{\dot{\phi}_i},\ u_0=g^{\lambda_0},\ u_i=g^{\lambda_i} \mod p \qquad i=1,\ldots,n$$

【００７９】ここで数１４の各変数の値を、置換証明文４１１として出力する。

※【数１４】

$$v,\dot{v}_0,\dot{v}_i,w,\dot{w}_0,\dot{w}_i,v',\dot{u}_i,u_0,u_i \qquad i=1,\ldots,n$$

※

【００８０】［リスポンス生成ステップ４１２］暗号文と公開鍵４０１と同一変換証明文４０９と置換証明文４１１と復号文４０６とが入力され、チャレンジを数１５★の式により計算する。

【数１５】

$$c_i = H_i(g_0,g_j,m_0,m_j,\tilde{g}_0,\tilde{g}_j,\tilde{m}_0,\tilde{m}_j,$$
$$v,\dot{v}_0,\dot{v}_j,w,\dot{w}_0,\dot{w}_j,v',\dot{u}_j,u_0,u_j$$
$$j=1,\ldots,n) \quad , \quad i=1,\ldots,n$$

【００８１】次にリスポンスを、数１６の式により計算する。

【数１６】

$$r_\mu = \sum_{\nu=0}^{n}A_{\mu\nu}c_\nu \mod q \qquad \mu=0,\ldots,n$$

$$\lambda = \lambda_0 + \sum_{i=1}^{n}\lambda_i r_i r_i \mod q$$

【００８２】最後に、同一変換証明文と置換証明文とリスポンスとをシャッフル証明文４１３として出力する。

【００８３】［復号証明ステップ４１７］復号文４０６と復号用の秘密鍵４００とリスポンス生成ステップで生成されたチャレンジ４１４とが入力される。任意の
$\beta \in_R \mod q$
を選び、次に、数１７の式を計算する。

【数１７】

$$\zeta = \prod_{i=1}^{n}\tilde{g}_i^{c_i} \mod p$$
$$\eta = \zeta^{x'} \mod p$$
$$\eta' = \zeta^{\beta} \mod p$$
$$m_0^* = g_0^{\beta} \mod p$$

【００８４】次に、復号証明のチャレンジを、数１８の

式により計算する。

【数１８】

$$c' = H_0(\zeta, \eta, \eta', g_0, m_0', m_0'')$$

【００８５】次に、復号証明のリスポンスを

$r' = c' x' + \beta \mod q$

と計算する。最後に復号の証明文４１５として、

η、η'、m_0''、r'

を出力する。

【００８６】［証明文］同一変換証明文と置換証明文と＊10

$$c_i = H_i(g_0, g_j, m_0, m_j, \tilde{g}_0, \tilde{g}_j, \tilde{m}_0, \tilde{m}_j, v, \dot{v}_0, \dot{v}_j, w, \dot{w}_0, \dot{w}_j, v', \dot{u}_j, u_0, u_j \quad j = 1, \ldots, n) \qquad i = 1, \ldots, n$$

＊リスポンスと復号証明文を、シャッフル復号の証明文４１６として出力する。

【００８７】［シャッフル復号検証］本実施の形態のシャッフル復号検証方法について、図３を参照して説明する。

【００８８】［同一変換検証ステップ］シャッフル復号証明文４１６と暗号文と公開鍵４０１と復号文が入力される。チャレンジ５００を、数１９の式により計算する。

【数１９】

$$c_i = H_i(g_0, g_j, m_0, m_j, \tilde{g}_0, \tilde{g}_j, \tilde{m}_0, \tilde{m}_j, v, \dot{v}_0, \dot{v}_j, w, \dot{w}_0, \dot{w}_j, v', \dot{u}_j, u_0, u_j \quad j = 1, \ldots, n) \qquad i = 1, \ldots, n$$

【００８９】次に、数２０の式が成り立てば「正当」を、成り立たなければ「不当」を出力５０１する。

【数２０】

$$\prod_{\mu=0}^{n} g_\mu^{r_\mu} = \prod_{\nu=0}^{n} \tilde{g}_\nu^{c_\nu} \mod p$$

$$\prod_{\mu=0}^{n} m_\mu^{r_\mu} = \eta \prod_{\nu=0}^{n} \tilde{m}_\nu^{c_\nu} \mod p$$

※【００９０】［置換検証ステップ］シャッフル復号証明文と同一変換検証ステップで求められたチャレンジ５００が入力される。次に、数２１の式が成り立てば「正当」を、成り立たなければ「不当」を出力５０２する。

【数２１】

※

$$u^\lambda = \dot{u}_0 \prod_{i=1}^{n} \dot{u}_i^{r_i r_i} \mod p$$

$$v'^\lambda v^{r0} g^{\sum_{i=1}^{n}(r_i^3 - c_i^3)} = \dot{v}_0 \prod_{i=1}^{n} \dot{u}_i^{c_i^2} \prod_{i=1}^{n} \dot{v}_i^{c_i} \mod p$$

$$w^{r0} g^{\sum_{i=1}^{n}(r_i^2 - c_i^2)} = \dot{w}_0 \prod_{i=0}^{n} \dot{w}_i^{c_i} \mod p$$

$$g_0^{r'} = m_0'^{c'} m_0'' \mod p$$

$$(\prod_{i=1}^{n} \tilde{g}_i^{c_i})^{r'} = \eta^{c'} \eta' \mod p$$

【００９１】［復号検証ステップ］シャッフル復号証明文と同一変換検証ステップで求められたチャレンジ５００が入力される。次に、補助のチャレンジを次の数２２の式により計算する。

【数２２】

$$c' = H_0(\zeta, \eta, \eta', g_0, m_0', m_0'')$$

【００９２】次に、数２３の式が成り立てば「正当」を、成り立たなければ「不当」を出力５０３する。

【数２３】

【００９３】同一変換検証ステップと置換検証ステップと復号検証ステップとの、全ての出力が正当であれば「正当」を、一つでも「不当」があれば「不当」を、シャッフル復号検証の出力５０４とする。

【００９４】なお、本実施の形態の証明付シャッフル復号システムは、証明付シャッフル復号装置１０のシャッフル部１１、復号部１２、証明部１３、同一変換証明部１３－１、置換証明部１３－２、リスポンス生成部１３－３、復号証明部１３－４の機能や、シャッフル復号検

証装置２０の同一変換検証部２１、置換検証部２２、復号検証部２３の機能や、その他の機能をハードウェア的に実現することは勿論として、各機能を備えるコンピュータプログラムである証明付シャッフル復号プログラム及びシャッフル復号検証プログラムを、コンピュータ処理装置のメモリにロードされることで実現することができる。この証明付シャッフル復号プログラム及びシャッフル復号検証プログラムは、磁気ディスク、半導体メモリその他の記録媒体８０、９０に格納される。そして、その記録媒体からコンピュータ処理装置にロードされ、コンピュータ処理装置の動作を制御することにより、上述した各機能を実現する。

【００９５】以上好ましい実施の形態及び実施例をあげて本発明を説明したが、本発明は必ずしも上記実施の形態及び実施例に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。

【００９６】

【発明の効果】以上説明したように本発明によれば、証明付シャッフルに証明付復号を追加した場合の計算量を、従来の技術と比べて大きく削減することができる。

【００９７】例えば、入力暗号文の数をｎとした時、文献２の従来技術を用いて証明付シャッフルに証明付復号を追加した場合には、乗剰余演算が３ｎ回必要とされていたのに対して、本発明によれば冪乗剰余演算はｎ＋３回で済み、従来の技術よりも大幅に冪乗剰余演算の回数を削減することができる。

【００９８】更に、本発明において行う冪乗剰余は、従来の技術における個別の冪乗剰余演算ではなく、冪乗剰余演算の積の計算であることから、個別の冪乗剰余演算よりも遥かに少ない計算量で計算することができ、更なる高速化を実現することができる。

＊【図面の簡単な説明】

【図１】　本発明の一実施の形態による証明付シャッフル復号システムの構成を示すブロック図である。

【図２】　本発明の一実施の形態による証明付シャッフル復号システムの処理を説明するためのフローチャートである。

【図３】　本発明の一実施の形態による証明付シャッフル復号を説明するための図である。

【図４】　本発明の一実施の形態によるシャッフル復号検証を説明するための図である。

【図５】　従来の技術における処理を説明するためのフローチャートである。

【図６】　従来の証明付シャッフルの処理を説明するための図である。

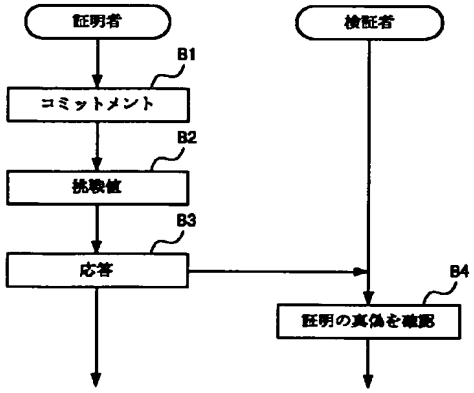
【図７】　従来の証明付復号の処理を説明するための図である。

【図８】　図６と図７の従来の技術を組み合わせた構成を示す図である。

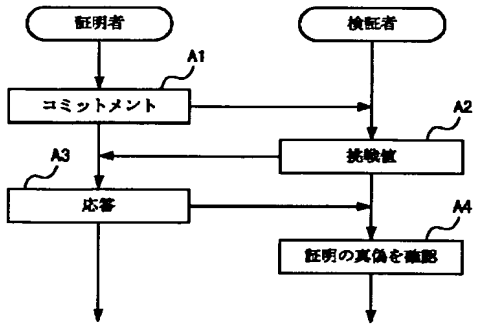
【符号の説明】

１０　証明付シャッフル復号装置
１１　シャッフル部
１２　復号部
１３　証明部
１３－１　同一変換証明部
１３－２　置換証明部
１３－３　リスポンス生成部
１３－４　復号証明部
２０　シャッフル復号検証装置
２１　同一変換検証部
２２　置換検証部
２３　復号検証部
８０、９０　記録媒体

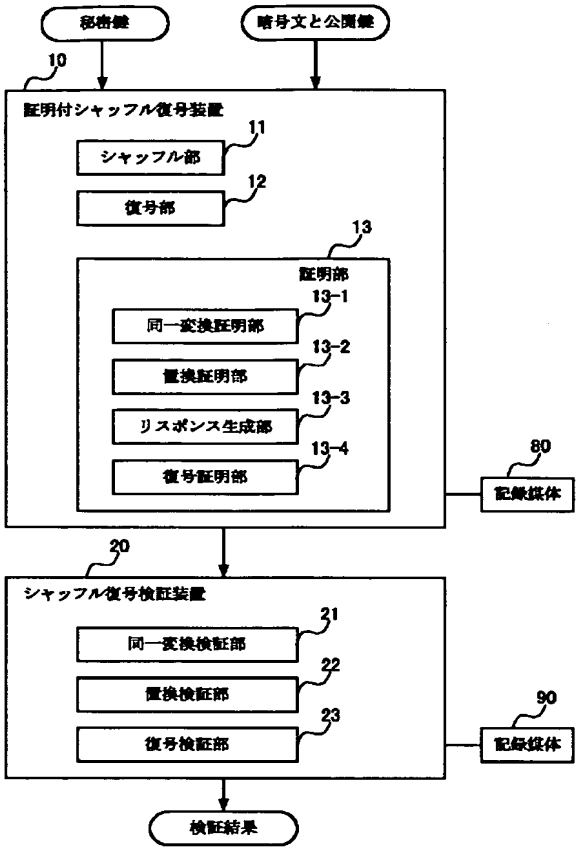
【図２】



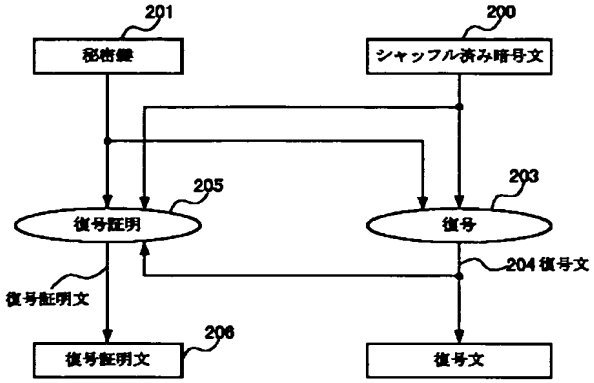
【図５】



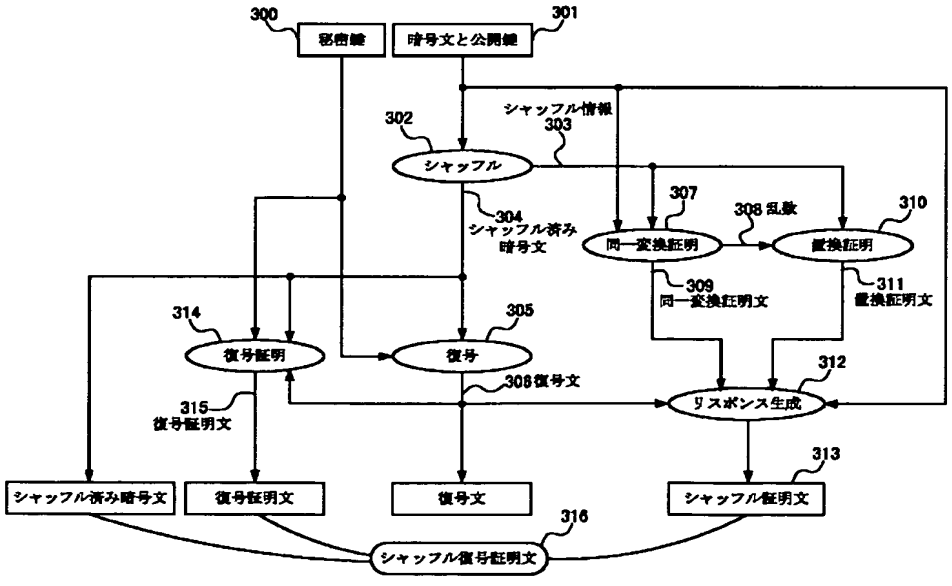
【図１】


秘密鍵
暗号文と公開鍵
10
証明付シャッフル復号装置
11
シャッフル部
12
復号部
13
証明部
13-1
同一変換証明部
13-2
置換証明部
13-3
リスポンス生成部
13-4
復号証明部
80
記録媒体
20
シャッフル復号検証装置
21
同一変換検証部
22
置換検証部
23
復号検証部
90
記録媒体
検証結果

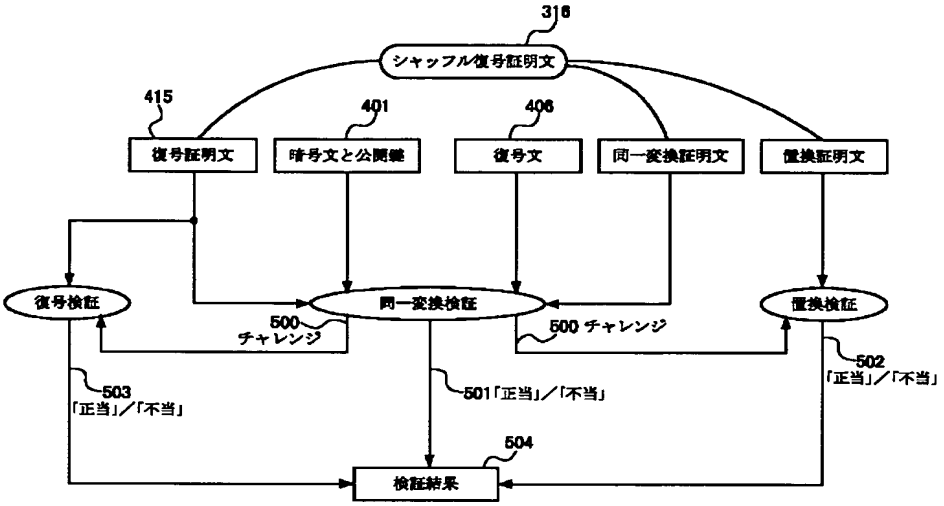
【図７】


201
秘密鍵
200
シャッフル済み暗号文
205
復号証明
203
復号
204 復号文
復号証明文
206
復号証明文
復号文

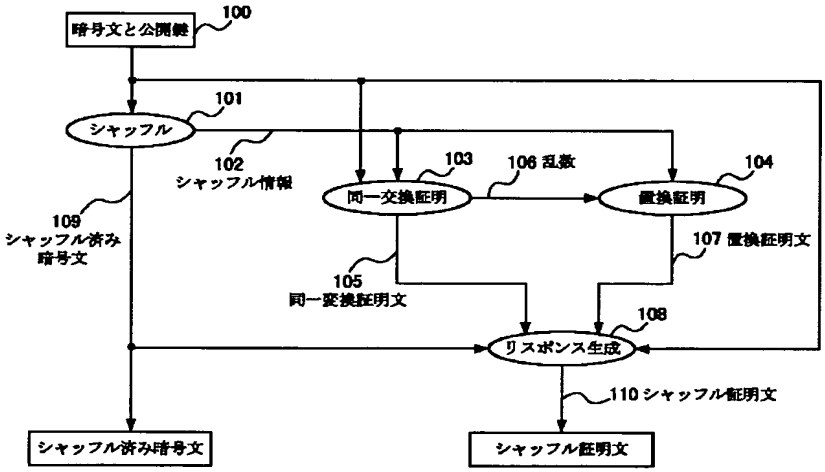
【図３】


300
秘密鍵
301
暗号文と公開鍵
302
シャッフル情報
303
シャッフル
304
シャッフル済み暗号文
307
同一変換証明
308 乱数
310
置換証明
309
同一変換証明文
311
置換証明文
314
復号証明
305
復号
308 復号文
312
リスポンス生成
315
復号証明文
313
シャッフル証明文
シャッフル済み暗号文
復号証明文
復号文
316
シャッフル復号証明文

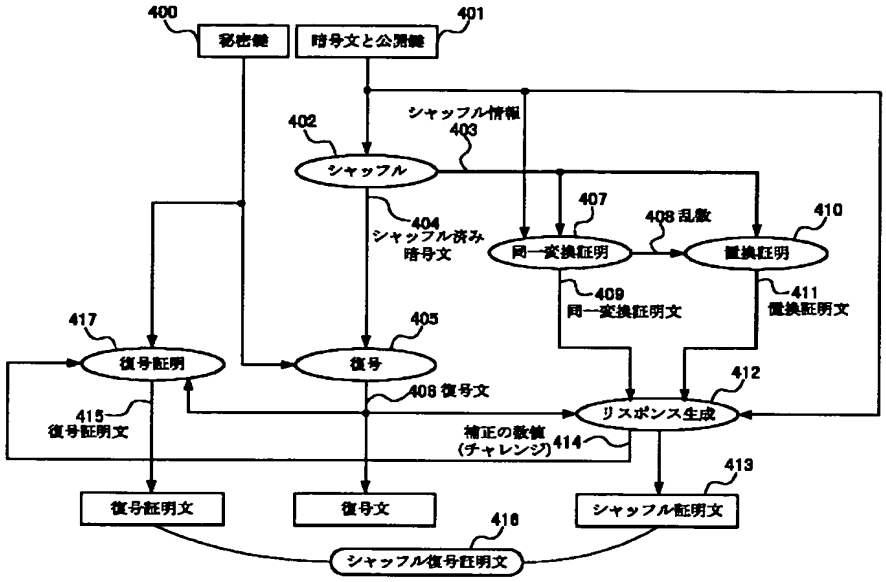
【図４】


316
シャッフル復号証明文
415
401
406
復号証明文
暗号文と公開鍵
復号文
同一変換証明文
置換証明文
復号検証
同一変換検証
置換検証
500
チャレンジ
500 チャレンジ
502
「正当」／「不当」
503
「正当」／「不当」
501「正当」／「不当」
504
検証結果

【図６】


暗号文と公開鍵
100
101
シャッフル
102
シャッフル情報
103
106 乱数
104
同一変換証明
置換証明
109
シャッフル済み
暗号文
107 置換証明文
105
同一変換証明文
108
リスポンス生成
110 シャッフル証明文
シャッフル済み暗号文
シャッフル証明文

【図８】


400
秘密鍵
401
暗号文と公開鍵
402
シャッフル
シャッフル情報
403
404
シャッフル済み
暗号文
407
同一変換証明
408 乱数
410
置換証明
409
同一変換証明文
411
置換証明文
417
復号証明
405
復号
408 復号文
412
リスポンス生成
415
復号証明文
補正の数値
(チャレンジ)
414
413
復号証明文
復号文
シャッフル証明文
416
シャッフル復号証明文